数理解析研究所講究録
第1873巻 2014年 158-162

A secret sharing scheme utilizing hyper graph

Tomoko Adachi
Department of Information Sciences, Toho University
2-2-1 Miyama, Funabashi, Chiba, 274-8510, Japan
E-mail: adachi@is.sci.toho-u.ac.jp

1. Introduction

A secret sharing scheme was introduced by Shamir in 1979 [10] and Blakley in 1979 [3] independently. This scheme has been studied by many scientists until today. Now, a secret sharing scheme has some important application to several areas of the information security. In Japan, NRI (Nomura Research Institute) Secure Technologies which is one of the private sector in the area of the information security, has provided clients with some cloud computing product named Secure Cube, from October in 2010. This cloud computing product is utilized by a secret sharing scheme, and is one good example of the application to an external storage unit.

The secret sharing scheme is a method to distribute shares of a secret value K among a set of participants P such a way that only the qualified subsets of P are able to reconstruct the value of K from their shares. In 1979, Shamir [10] introduced the secret sharing scheme which was based Lagrange's interpolation formula. This scheme is called Shamir's threshold scheme. In 1992, Pedersen [9] applied a verifiable secret sharing scheme to Shamir's threshold scheme.

Since the security of a system depends on the amount of information that must be kept secret, the size of the shares given to the participants is key point in the design of secret sharing schemes. Hence, the information rate is an important criterion for measure to a secret sharing scheme.

There are two methods of construction about a secret sharing scheme. One is utilized the n dimensional vector space, and the other is utilized the graph theory. The former is introduced by Brickell in 1989 [4]. In 1998, Padro [8] adopted a verifiable secret sharing scheme utilizing the n dimensional vector space. In the case of the latter, there are many studies. A secret sharing scheme related to graph decomposition is studied by Stinson in 1994 [11], and by Blundo et. al. in 2003 [2]. A secret sharing scheme by Farre and Padro in 2006 [7] adopt an access structures with intersection number equal to one. Moreover, it is also related to hyper graph decomposition, as introduced by Crescenzo and Galdi in 2009 [6]. An information rate is one of the main parameters in secret sharing.

The information rate is studied by Brickell and Stinson in 1992 [5], and by C.Blundo et. al. in 1993 [1].

In this paper, we describe a secret sharing scheme utilizing a graph, and utilizing a hyper graph.

2. Graph based secret sharing scheme

In this section, at first, we describe some graph-theoretic definitions which we need. Secondly, we define the information rate. Finally, we describe a secret sharing scheme utilizing a hyper graph.

We think of a graph as a set of points in a plane or in 3-space and a set of line segments, each of which either joins two points or joins a point to itself. A graph G is a pair $G = (V, E)$ consisting of two finite sets V and E. The elements of V are called a vertices, and the elements of E are called an edges. The notations $V(G)$ and $E(G)$ are used for the vertex-set and edge-set of G, respectively. Each edge has a set of one or two vertices associated to it, which are called its endpoints.

A hyper graph is a generalization of a graph in which an edge can connect any number of vertices. a hyper graph H is a pair $H = (X, E)$, where X is a set of elements called vertices, and E is a set of non-empty subsets of X called hyper edges. Hence, E is a subset of $\mathcal{P}(X) \setminus \{\phi\}$, where $\mathcal{P}(X)$ is the power set of X. While each edge of a graph has a set of one or two vertices, each hyper edge of a hyper graph has arbitrary sets

of vertices, and can therefore contain an arbitrary number of vertices. The notations $V(H)$ and $E(H)$ are used for the vertex-set and the hyper edge-set of H, respectively.

Suppose that P is a set of participants, and $K \in GF(q)$ is a secret value. Let S be a set of size q containing all the possible secrets to be shared. We denote by s the random variable taking values in S according to the distribution probability. For every participant $P_i \in P$ $(1 \leq i \leq n)$, let us denote by S_{P_i} the set containing all the possible information given to P by a secret sharing scheme. The elements in S_{P_i} are called shares. As appears in the literature, we will denote by P both the player in the access structure and the random variable describing shares assigned to him. Suppose a dealer wants to share a secret among the participants in P. For each player in P, he selects one element in S_{P_i} according to some.

Now, we will use the value ρ for measuring of a secret sharing scheme, that is, the information rate. It depends on the amount of information distributed to the participant.

Definition 2.1 . *The information rate ρ is defined as follows:*

$$\rho = \frac{H(K)}{\max_{P_i \in P} H(P_i)}, \tag{2.1}$$

where $H(K)$ is an entropy of a secret value K and $H(P_i)$ is an entropy of a participant P_i.

When the probability distributions over the secrets and the shares are uniform, the information rate reduces to the following.

$$\rho = \frac{\ln q}{\max_{P_i \in P} \ln S_{P_i}}. \tag{2.2}$$

Definition 2.2 . *The optimal information rate ρ^* can be defined as follows:*

$$\rho^* = \sup \rho. \tag{2.3}$$

Here, we describe a secret sharing scheme utilizing a graph $G = (V, E)$. We obtain the following theorem, since we correspond the vertex set $V(G)$ to the set of participants P, and each edge to a reconstruct-able set of participants.

Theorem 2.1 . *Any graph corresponds to a secret sharing scheme.*

Similarly, for a hyper graph $H = (V, E)$. we obtain the following theorem. Because we correspond the vertex set $V(H)$ to the set of participants P, and each hyper edge to a reconstruct-able set of participants.

Theorem 2.2 . *Any hyper graph corresponds to a secret sharing scheme.*

参考文献

[1] C. Blundo, A. D. Santis, L. Gargano and U. Vaccaro, Graph Decompositions and Secret Sharing Schemes. *Advances in Cryptology — CRYPTO' 92 ,Lecture Notes in Computer Science*, vol. **740** (1993), pp. 148–167.

[2] C. Blundo, A. D. Santis, D. R. Stinson and U. Vaccaro, Graph Decompositions and Secret Sharing Schemes. *Journal of Cryptology*, vol. **8** (2003), pp. 39–64.

[3] G. R. Blakley, Safeguarding cryptographic keys. *AFIPS Conference Proceedings*, vol. **48** (1979), pp. 313–317.

[4] E. F. Brickell, Some ideal secret sharing schemes. *Journal of Combinatorial Mathematics and Combinatorial Computing*, vol. **6** (1989), pp. 105–113.

[5] E. F. Brickell and D. R. Stinson, Some improved bounds on the information rate of prefect secret sharing schemes. *Journal of Cryptology*, vol. **5** (1992), pp. 153–166.

[6] G. D. Crescenzo and C. Galdi, Hypergraph decomposition and secret sharing. *Discrete Applied Mathematics*, vol. **157** (2009), pp. 928–946.

[7] J. M. Farre and C. Padro, Secret sharing schemes on access structures with intersection number equal to one. *Discrete Applied Mathematics*, vol. **154** (2006), pp. 552–563.

[8] C. Padro, Robust vector space secret sharing schemes. *Information Processing Letters*, vol. **68** (1998), pp. 107–111.

[9] T. P. Pedersen, Non-Interactive and information-Theoretic Secure Verifiable Secret Sharing. *Advances in Cryptology CRYPTO' 91*, (1992), pp. 129–140.

[10] A. Shamir, How to share a secret. *Communications of the ACM*, vol. **22** (1979), pp. 612–613.

[11] D. R. Stinson, Decomposition constructions for secret sharing schemes. *IEEE Transactions on Information Theory*, vol. **40** (1994), pp. 118–125.